REMARKS/ARGUMENTS

The present application discloses a document repository system in which the originator of the document is able to ensure the integrity and security of its document filed with a third party repository without having to trust the administrator of that repository. In this repository system, the document originator and the repository administrator have vault environments which are secure extensions of their respective work spaces. The vault of the document originator encrypts a document that it receives from the originator, prior to forwarding it on to the vault of the repository to maintain the document secure from the repository administrator. When a request is made to view the document, it is made from the vault which is a secure extension of the requesting party's work space to the repository's vault. The repository's vault retrieves a copy of the encrypted document which is forwards, along with the requester's identity, to the originator's vault. The originator's vault verifies that the requester is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself. The originator's vault decrypts the document and forwards the decrypted document directly to the requester's vault. Therefore the repository administrator never handles the decrypted documents or the encrypting and decrypting of the documents.

The repository system also maintains the information on authorized user access secure from any actions of the third party administrator of the repository. To this end, the system includes a communications environment that houses a first agent program in the data repository system which is a

secure extension of the work space of the depositor's computer and a second agent program which is a secure extension of the work space of a first user computer with access privileges to the electronic data file. A manifest is accessible to and maintained by the first agent program. The first user computer has a record of its access privileges to the electronic data file which is accessible to and maintained by the second agent program. When changes are made to the manifest affecting the first user computer's access privileges to the electronic data file, these changes are communicated from the first agent program to the second agent program so that the first user computer's record of its access privileges can be updated. The first agent program is also able to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program.

Claim Rejections Under 35 USC 102

A. Original claims 1 to 6, 12, 13, 22 and 23, in the application were all rejected under 35 USC 102(e) as being anticipated by the Carroll, U.S. patent, #6,105,131.

The applicant's attorney did not find where the Carrroll patent discloses preventing access by the repository administrator to either the vault owners vault or a directory of authorized users of data stored in the repository. In fact, contrary to the Examiner's position, Carroll specifically provides a repository administrator to have access to the vault space. Lines 60 to 66 of Carroll provide that "only the vault owner ... and the system administrator can access the disk space" of a personal vault (emphasis added). The Carroll patent relies

on the information in the vault being "unintelligible to the system administrator" because it is "encrypted" not because access limitations placed on the system administrator since the system administrator has access.

Claims 1 to 6, 12, 13, 22 and 23 are not anticipated by the Carroll patent.

For instance, independent claim 1 calls for a secure electronic data storage and retrieval system having having means in an environment maintained secure from the repository manager to decrypt electronic data on request of a requesting computer. The Carroll patent in Figure 6 and column 9, beginning on line 14, makes it clear that the user terminal is granted access to secure data and it is not inherent in the description that the agent program of a depositing computer decrypts encrypted data and provides the decrypted data to a different requesting computer.

Claims, dependent of claim 1, further distinguish over the prior art.

For instance in claim 2, the repository manager is adapted to digitally sign the encrypted data prior to storage and the agent program of the depositing computer is adapted to verify in the environment secure from the repository manager against the signed encrypted data data following decryption.

Claim 3 further distinguishes over the Carroll reference in that the agent program is adapted to forward decrypted electronic data directly from the environment secure from the repository manager to the requesting computer without providing access to the repository manager.

Claim 4 further distinguishes in that the agent program is a secure extension of the depositing computer and is adapted to manage computer communications between the depositing computer and repository manager.

Claim 5 further distinguishes in that it calls for housing the agent program of the depositing computer and a secure extension of the repository manager and environments adapted to manage communications.

Independent claim 12 calls for storing encrypted electronic data in an electronic repository in an environment free from access by the data repository manager. As pointed out previously, the Carroll patent says the system administrator can access the vault space.

Claims dependent on claim 12 further distinguish over the prior art.

For instance, claim 13 further distinguishes in that it calls for the source to provide decrypted data directly to the requesting user without providing access to the data repository manager.

Claim 14 calls for an access control list of user authorizations associated with the electronic data that is stored in a repository in the environment free from access by the repository manager.

Independent claim 22 calls for computer software for storing encrypted electronic data and deposit receipt in a data repository free from access by the repository manager.

Dependent claim 23 calls for the computer software product of claim 22 having software for retrieving and decrypting encrypted data and sending it directly to the requesting user without providing access to the repository manager.

For the above reasons all claims 1 to 6, 12, 13, 22 and 23 patentably distinguish from the Carroll reference. Since these claims patentably distinguish from the Carroll reference, they were improperly rejected under 35 USC 102. As for rejection under 35 USC 103, it is pointed out that section 35 USC 103(c) specifically excludes the Carroll reference from being prior art under 103 since the Carroll reference and the present application were both owned or obligated to be assigned, to the assignee of the present application at the time of the invention thereof. The Carroll patent states that it is assigned to IBM. The enclosed assignment shows that this application is assigned to IBM. To eliminate any issue of double patenting, the applicant have included a Terminal Disclaimer disclaiming the terminal portion of any patent which may issue on the above identified application.

B. Original claims 7, 8, 14 to 18, 25 and 26 were rejected under 35 USC 102(e) as being anticipated by Chiu, U.S. Patent #6,181,336.

Applicant's attorney did not find where the Chiu patent teaches preventing access by the system administrator to a vault owners vault. In fact, it appears from lines 7 to 24 of column 24, that system administrators have control over access to objects through control over who has access to a users

vault by changing the ACLs. Therefore in Chiu, an administrator has access through the ability to change the ACLs granting access to the users vault.

Claims 7, 8, 14 to 18, 25 and 26 all distinguish from the Chiu patent for the above reasons. For instance, independent claim 7 calls for authenticating access to electronic data using an access control list stored in a repository environment secure from the repository manager and allowing updates to the access control list only from the source of the electronic data.

Independent claim 17 distinguishes over the prior art in that it calls for a computer program product for authenticating user access to electronic data stored in a data repository secure from a repository manager with access control lists of user authorizations stored in the data repository in an environment secure from access of the repository manager.

Claim 24 further distinguishes for associating an access control list of authorized authorizations along with the electronic data in a data repository free from access by the repository manager in data repository in areas free from access by the data manager.

Rejections Under 35 USC 103

Original claims 9 to 11, 19 and 21 where rejected under 35 USC 103(a) as being unpatentable over Chiu in view of Carroll.

Since, as pointed out in A, under 35 USC 103(c) the Carroll patent is not a proper reference against the present application under 35 USC 103, claims 9 to 11, 19 and 21 are allowable over the cited combination. Further, since, as pointed out above, neither the Chiu or Carroll patents excludes access to the vaults of the data suppliers or users or prevents access to the access list, the combination of these two patents does not.

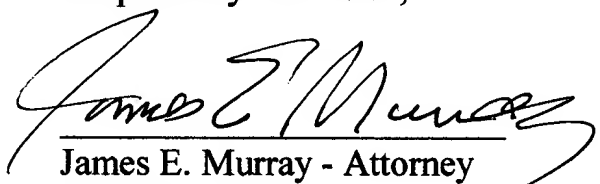
For the above reasons all claims in the application are allowable over the cited references. Independent claims 1, 7, 12, 17 and 22 all call for having portions of a data repository where data and/or control lists are maintained secure from the repository administrator.

Changes to the Specification

A number of corrections have been made to the specification. For instance, the application # of the copending application has been added to page 1. The referral to "Figure 4" on page 12, has been changed to -- Figures 4A and 4B -- which are the figures contained in the drawings. Also, grammar of the paragraph beginning on page 5, line 29, and other paragraphs, has been corrected.

For the above reasons, it is respectfully submitted that the claims are allowable over the prior art and the application is in condition for allowance. Therefore, it is requested that the application be reconsidered, allowed and passed to issue.

Respectfully submitted,



James E. Murray - Attorney
Reg. No.: 20,915
Telephone No.: (845) 462-4763